



Richard K. Herrmann
302.888.6816
rherrmann@morrisjames.com

April 25, 2008

VIA EFILING AND HAND DELIVERY

The Honorable Sue L. Robinson
United States District Court
District of Delaware
844 King Street
Wilmington, Delaware 19801

Re: SRI International v. ISS and Symantec, D. Del., C.A. No. 04-1199-SLR

Your Honor:

Symantec submits this letter in response to the Court's request for a short letter prior to the status conference scheduled for April 29. Symantec urges the Court to rule as a matter of law upon a single obviousness combination that was left unaddressed by the Court's prior summary judgment rulings.

Defendants previously asserted that the *Emerald 1997* reference in combination with its internally-cited reference *Intrusive Activity 1991* rendered all of the asserted claims of the '203 and '615 patents obvious.¹ The Federal Circuit's decision affirming that the *Emerald 1997* reference anticipates the '212 patent precludes SRI from relitigating the fact that *Emerald 1997* satisfies all the limitations of the '212 claims. Due to the substantial overlap between the '212, '203 and '615 patent claims, only a single limitation remains at issue for all asserted claims of the '203 and '615 patents. Summary judgment on this issue would resolve all remaining claims against Symantec.

As shown in the chart below, claim 1 of the '212 and '203 patents differ by only a single limitation (shown in bold) relating to certain categories of network traffic data.²

¹ See D.I. 297 at 30-32 discussing the combination of *Emerald 1997* with *Intrusive Activity 1991*.

² All of the remaining asserted claims, including the '615 claims, similarly differ by only this single limitation.

The Honorable Sue L. Robinson
 April 25, 2008
 Page 2

Morris James LLP

'212 Claim 1	'203 Claim 1
Method for monitoring an enterprise network, said method comprising the steps of:	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:
deploying a plurality of network monitors in the enterprise network;	deploying a plurality of network monitors in the enterprise network;
detecting, by the network monitors, suspicious network activity based on analysis of network traffic data,	detecting, by the network monitors, suspicious network activity based on analysis of network traffic data
	selected from the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet};
generating, by the monitors, reports of said suspicious activity; and	generating, by the monitors, reports of said suspicious activity; and
automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.

Thus, the only issue remaining is whether: (1) *Intrusive Activity 1991* disclosed one of the claimed categories of network traffic data, and (2) there was a reason to combine *Emerald 1997* with *Intrusive Activity 1991*.

The parties have conferred, and Symantec believes that this issue can be decided by relying upon two facts which are undisputed: (1) the *Intrusive Activity 1991* reference specifically described detecting suspicious network activity using one of the claimed categories of network traffic data;³ and (2) the *Emerald 1997* reference discussed and cited to the *Intrusive Activity 1991* reference, demonstrating a reason to combine them.

Unable to dispute these facts, SRI nevertheless claims there is a genuine dispute of material fact. SRI claims there is contrary expert testimony about the meaning of the disclosure in *Intrusive Activity 1991*, and SRI points to allegations of secondary considerations. But as the recent *KSR* Supreme Court case makes clear, SRI cannot manufacture a material dispute of fact

³ For example, *Intrusive Activity 1991* specifically disclosed analysis of the claimed network traffic data category "network packet data volume" which satisfies the only remaining '203 and '615 limitation: "This simple definition of a process has a simple identifier, *stream*, addresses for the source and destination hosts, source and destination ports to specify the processes on the two machines, a time of creation, **the number of packets exchanged between the two processes**, and **the number of bytes in all the packets exchanged**." *Id.* at 368.

The Honorable Sue L. Robinson
April 25, 2008
Page 3

Morris James LLP

merely by pointing to unsupported expert testimony of non-obviousness, or secondary considerations.⁴

In light of the Federal Circuit's binding determination, the two relevant undisputed facts, and the *KSR* decision, Symantec believes the Court would benefit from further briefing on this issue, because this case is ripe for resolution by summary judgment. In the alternative, Symantec urges the Court to rule upon its pending summary judgment motions, in particular the one identified herein.

We look forward to our hearing with you on Tuesday.

Respectfully,

/s/ Richard K. Herrmann

Richard K. Herrmann, I.D. No. 405
rherrmann@morrisjames.com

RKH/tp

cc (w/encl): Dr. Peter T. Dalleo, Clerk of the Court (via hand delivery)
John Horvath, Esq. (via email)
Howard G. Pollack, Esq. (via email)
Richard L. Horwitz, Esq. (via email)
David Moore, Esq. (via email)
Holmes Hawkins, III, Esq. (via email)

⁴ See *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1746-47 (2007).